AMENDMENTS TO THE CLAIMS:

1.   (Currently Amended) An input device for securing a token from an unauthorized user:

a user interface for accepting entry of a personal identifier from a user, the user interface being communicatable with a host processing device and being different from a keyboard associated with the host processing device;

a processor, communicatively coupled to the user interface;

a token interface, including:

a token interface emitter, for producing a signal having information including the personal identifier, the token interface emitter communicatively coupled to the processor and further communicatively coupled to a token sensor when the token is physically coupled with the token interface, the signal produced by the token interface emitter being sent to and received by the token; and

a physical shield, substantially opaque to the wavelength of the signal, for substantially confining reception of the signal to the token sensor.

2.   (Original) The input device of claim 1, wherein the token interface emitter is communicatively decoupled from the token sensor when the token is not physically coupled with the token interface.

3.   (Original) The input device of claim 1, wherein the token interface includes a USB port.

4.   (Original) The input device of claim 1, wherein the shield substantially circumscribes the token interface emitter.

5.   (Original) The input device of claim 1, wherein the token interface further comprises:

2

a token interface sensor configured to receive the signal produced by a token emitter when the token is physically coupled with the token interface.

6.　　(Original)　The input device of claim 5, wherein the token emitter emits a second signal including information describing the intensity of the signal.

7.　　(Original)　The input device of claim 6, wherein the processor controls the intensity of the first signal according to the information describing intensity of the first signal received from the second signal.

8.　　(Currently Amended)　A method of securing a token having a USB-compliant interface from unauthorized use, comprising the steps of:

accepting the token in an input device having a token interface, the input device being communicatable with a host processing device and being different from a keyboard associated with the host processing device;

accepting a user-entered personal identifier in the input device; ~~and~~

transmitting the user-entered personal identifier to the token via a communication path distinct from the USB-compliant interface by generating a first signal having information including the user-entered personal identifier, and emitting the generated signal in the token interface for reception by a token sensor; and

physically shielding the signal in a substantially opaque manner with respect to the wavelength of the signal to confine reception of the signal to the sensor.

9.　　(Cancelled)

10.　　(Currently Amended)　The method of claim ~~9~~ 8, further comprising the step of receiving the generated first signal in a token sensor.

11.　　(Cancelled)

12.　　(Currently Amended)　The method of claim ~~9~~ 8, wherein:

3

the method further comprises the step of determining if the token is accepted in the device; and

the user-entered personal identifier is transmitted to the token via a communication path independent from the USB-compliant interface only if the token is determined to be accepted by the input device.

13.   (Original) The method of claim 12, wherein the step of determining if the token is accepted in the input device comprises the step of sensing a connect signal.

14.   (Original) The method of claim 12, wherein the step of determining if the token has been accepted by the input device comprises the step of: receiving a second signal produced by a token emitter when the token is accepted by the token interface.

15.   (Original) The method of claim 12, wherein the step of determining if the token has been accepted by the input device comprises the step of:

receiving a second signal produced by a token emitter after the token sensor receives a third signal in the token interface.

16.   (Currently Amended) The method of claim 9 8, further comprising the steps of:

receiving a second signal produced by a token emitter, the second signal including information describing the intensity of the first signal; and

controlling the intensity of the first signal according to the information describing the intensity of the first signal received from the second signal.

17.   (Original) The method of claim 8, further comprising the steps of: disabling transmission of the user-entered personal identifier until detection of the acceptance of the token to the USB port.